Commonwealth Office of Technology Monthly Cyber Security Tips

October 2009 Volume 4, Issue 10

Top Ten Cyber Security Tips

From the Office of COT's Chief Information Security Officer

October is Cyber Security Awareness Month – Our Shared Responsibility

In recognition of the 2009 National Cyber Security Awareness Month, this edition of the newsletter is designed to provide you with the TOP 10 Cyber Security Tips that you can - and should - use to protect your computer system.

1. Think Before You Click

Always think before you click on links or images in an email, instant message, or on web sites. Be cautious when you receive an attachment from unknown sources. Even if you know and trust the sender of the email, instant message, web site, or a friend's social networking page, it is still prudent to use caution when navigating pages and clicking on links or images.

2. Use Hard to Guess Passwords

Developing good password practices will help keep your personal information and identity more secure. Passwords should have at least eight characters and include uppercase and lowercase letters, numerals and symbols.

3. Avoid Phishing Scams

Phishing is a form of identity theft in which the intent is to steal your personal data, such as credit card numbers, passwords, account data, or other information. Do not reply to emails that ask you to "verify your information" or to "confirm your user-id and password."

4. Shop Safely Online

When shopping online always know with whom you're dealing. When submitting your purchase information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission. Always remember to pay by credit card and keep a paper trail.

5. Protect Your Identity

When visiting web sites, it's important to know what information is being collected, by whom and how it will be used. Web sites track visitors as they navigate through cyberspace, therefore, data may be collected about you as a result of many of your online activities. Please keep in mind most legitimate web sites include a privacy statement. The privacy statement is usually located at the bottom of the home page and details the type of personally identifiable information the site collects about its visitors, how the information is used - including with whom it may be shared - and how users can control the information that is gathered.

6. Dispose of Information Properly

Before discarding your computer or portable storage devices, you need to be sure that the data contained on the device has been erased or "wiped." Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DOD) compliant software.

7. Protect Your Children Online

Discuss and set guidelines and rules for computer use with your child. Post these rules by the computer as a reminder. Familiarize yourself with your child's online activities and maintain a dialogue with your child about what applications they are using. Consider using parental control tools that are provided by some Internet Service Providers and available for purchase as separate software packages.

8. Protect Your Portable Devices

It is important to make sure you secure your portable devices to protect both the device and the information contained on the device. Always establish a password on all devices. If your device has Bluetooth functionality and it's not used, check to be sure this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, be sure to change the default password for connecting to a Bluetooth enabled device. Encrypt data and data transmissions whenever possible.

9. Secure Your Wireless Network

Wireless networks are not as secure as the traditional "wired" networks, but you can minimize the risk on your wireless network by enabling encryption, changing the default password, changing the Service Set Identifier (SSID) name (which is the name of your network) as well as turning off SSID broadcasting and using the MAC filtering feature, which allows you to designate and restrict which computers can connect to your wireless network.

10. Back-Up Important Files

Back-up your important files minimally on a weekly basis. Don't risk losing your important documents, images or files!

For more information on the Top 10 Cyber Security Tips,
please visit the MS-ISAC Monthly Cyber Security Newsletter Tips:
www.msisac.org/awareness/news/

Online Resources

To learn more about protecting information visit the following online resources:

- **MS ISAC Monthly Cyber Security Tips**: www.msisac.org/awareness/news
- **US CERT**: www.us-cert.gov/reading_room
- **OnGuard Online**: www.onguardonline.gov/topics.html
- **Privacy Rights Clearinghouse**: www.privacyrights.org

For more cyber security monthly tips go to:

www.msisac.org/awareness/news/
technology.ky.gov/security/CyberAwareness.htm

Brought to you by:

MS-ISAC

www.msisac.org

technology.ky.gov